SwA Forum – March 12, 2010

Open Group and OMG Update
& Discussion on Standards Harmonization

Andras Szakal
IBM Distinguished Engineer
Director Software Architecture
IBM Federal Software Group

Automated Compliance Expert – Working Group

Agenda

Update on Software Assurance Activities

- The Open Group
- Object Management Group

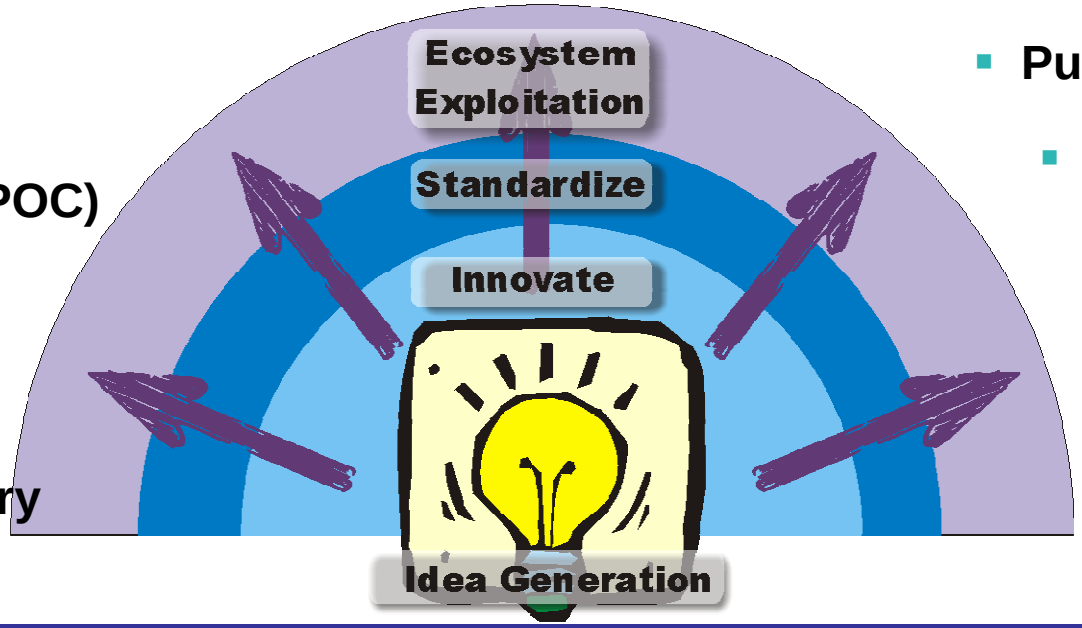
Harmonization

SMT

Standards Success Requires Broad Vision

The industry invests widely to develop and influence standards, enhance consumablity and drive standards-based business strategies.

- Early Customer Engagements
- Competitive Initiatives
- Intellectual Property
- Products
- Public Relations
- Early Code (POC)
- Standards Bodies
- Partners
- Industry Groups
- Competitors
- ISVs, Adjacent Standards
- Complementary



The value back to the end user and the industry is realized in Choice, **Flexibility**, Speed, Agility, Skills.

SMT

Open Group SwA Activities Overview

- **Compliance**
  - Automated Security Compliance Expert (ACE)
  - XDAS – Update of the Distributed Audit Service
  - ISM3 - Information Security Metrics/Maturity Model (ISM3)
- **Method**
  - TOGAF – Security Guidance
  - SOA Reference Architecture
  - SOA Security Guide
- **Cloud Security**
  - Cloud security standards / best practices
- **Cybersecurity**
  - Trustworthy Vendor Framework
- **Profession Certification**
  - IT Architect Profession Certification (ITAC)
  - IT Specialist Certification (ITSC)
    - ✓ITSC Security Stream

SMT

Automated Compliance Expert Requirements

Customer Collaboration and Requirement Gathering

- **Industry**
  - Financial
  - Medical
  - Entertainment
- **Consultants**
  - Auditors
- **Research**
- **Governance**

Customer Pain Points

- Cost of Compliance
  - Manual configuration
  - home-grown configuration scripts difficult to maintain and audit
- Companies and systems must meet multiple compliance regulations
  - PCI, SOX/COBIT, Internal Security Policies, US Gov.
- Compliance Audits:
  - Time consuming
  - Expensive
  - Auditors/Audits are not consistent

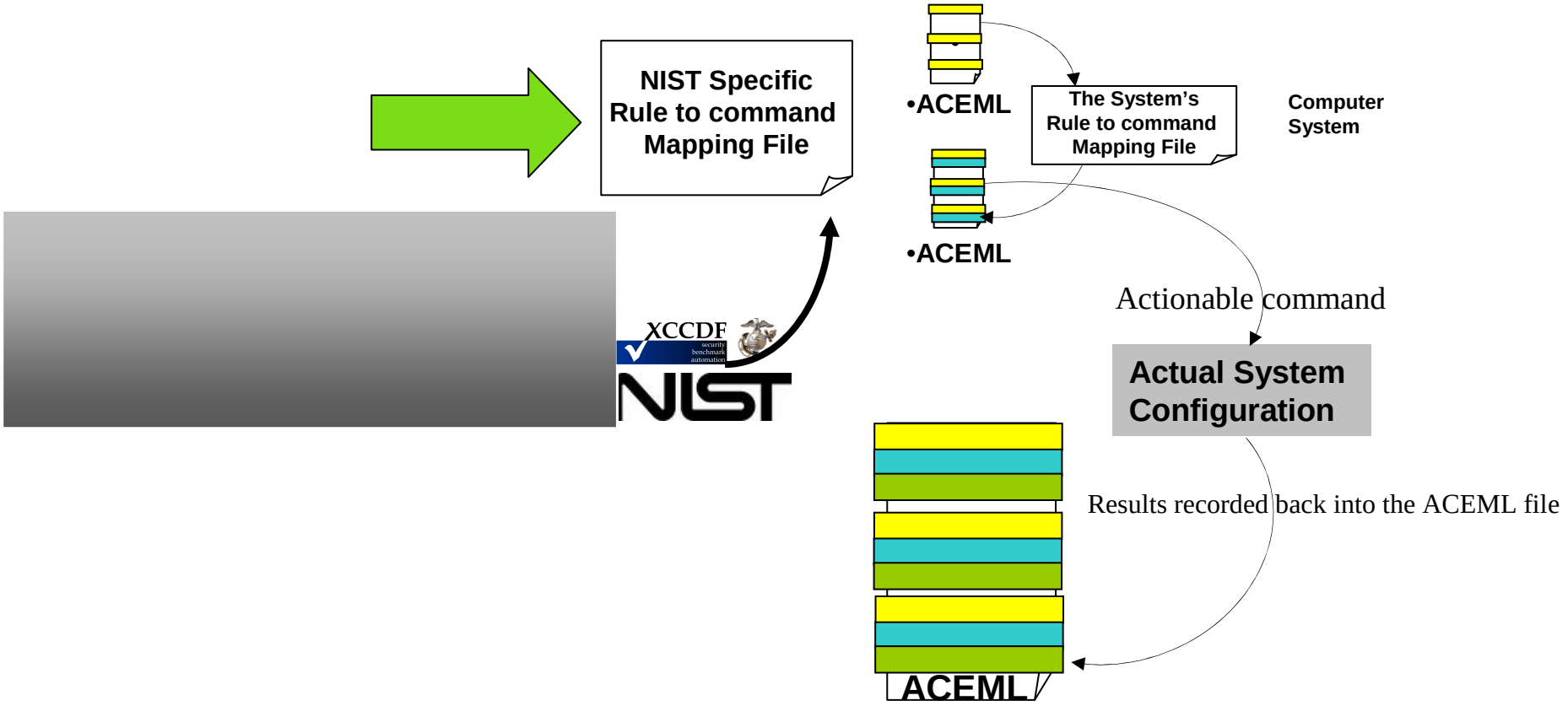
Desired Features

- Automated Security and Compliance Configuration
- Automated Monitoring
- Standardized Compliance
- Combines Multiple Compliance Requirements
- Platform Independent
- Complete Audit Reporting
- Compliance Over Ride and Policy Authoring

SMT

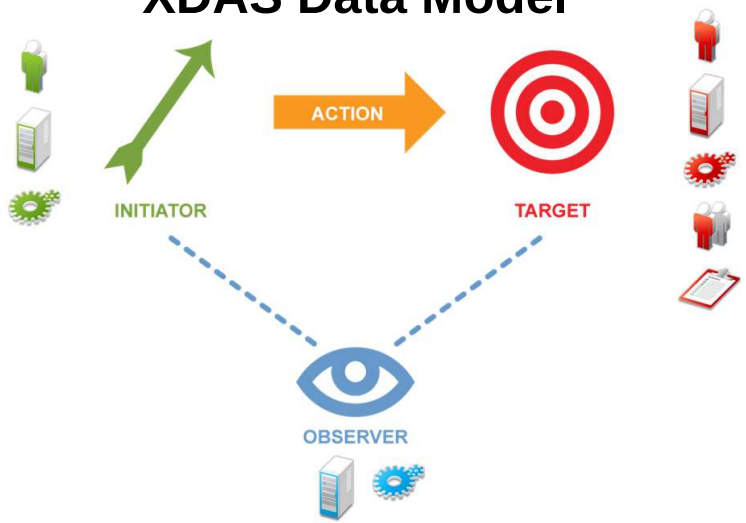
ACEML and SCAP Integration Point – Rule to Command Mapping

- Reconciliation of Policy Standards
- Blending Compliance Policy
- Authoring Tools



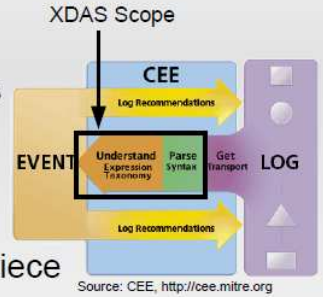
XDAS – Distributed Audit Service

XDAS Data Model



XDAS Positioning

- CEE (on going effort – MITRE)
  - Broader approach
    - Event generation recommendations
    - Event transportation
  - Many XDAS members are involved in CEE
  - XDAS could be one of the CEE piece

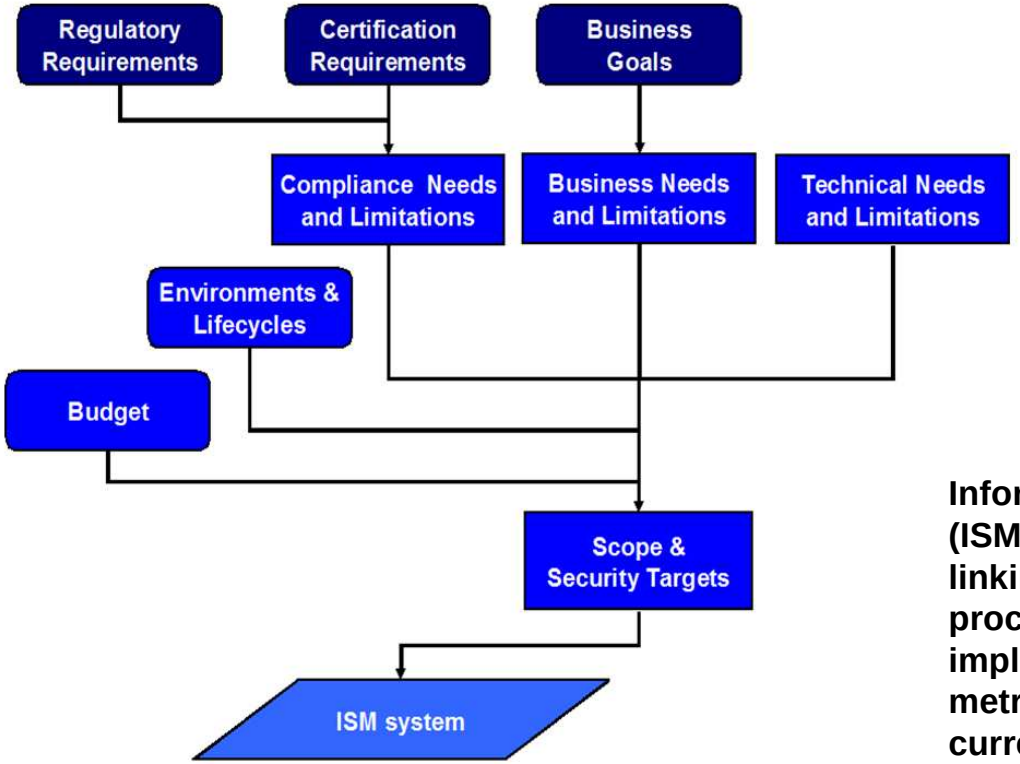


Source: CEE, http://cee.mitre.org

- IDMEF (RFC 4765)
  - Same data model concepts
  - Focused on Intrusion Detection Messages
  - No taxonomy

- **Effort to update the XDAS specification to be broadly applicable to today's cross platform architecture**
- **Focused on integration with SIEM tools**

ISM3 – Information Security Maturity Management Maturity Model



Information Security Metrics/Maturity Model (ISM3) Standard: Incorporating best practices for linking security to business needs, using a process-based approach, providing implementation guidance, and using specific metrics, while preserving compatibility with current IT and security management standards.

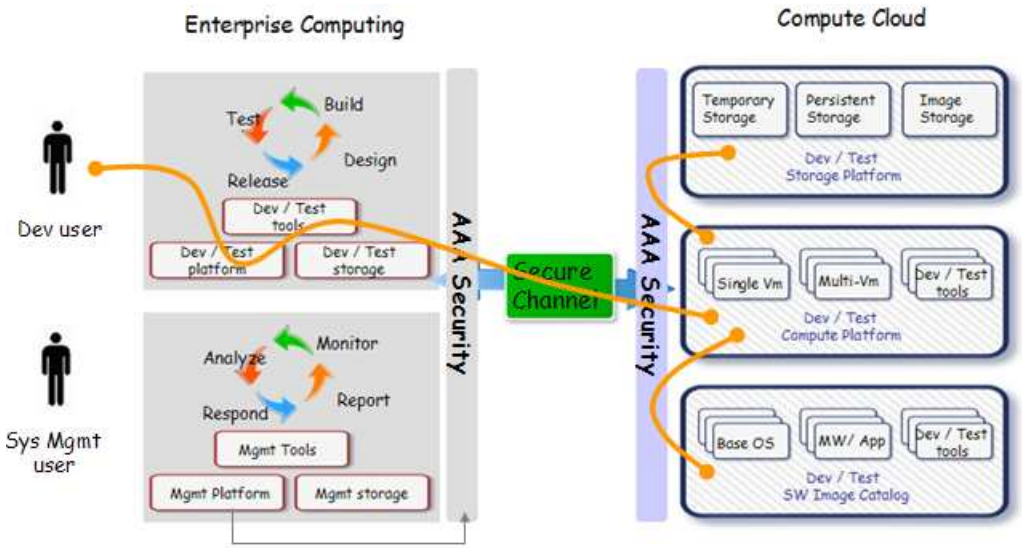
- **EU / Span based Security Operations Maturity Model**
- **Rationalize with other security maturity models**

Open Group Security and Assurance **Method** Standards Activities

- **Integration of Security into TOGAF**: Joint activity with the RT&ES Forum and SOA Working Group.
- **Enterprise Security Architecture (ESA) Guide**: Updating our 2004 ESA Guide.
- **COA Framework Standard:** Developing a standard for a Framework for Collaboration-Oriented Architectures.
- **Security Reference Architecture**: Developing a reference architecture,to demonstrate how to build secure EAs.
- **Cloud Security Reference Architecture Guide**: Joint activity with the Cloud Computing Working Group.
- **SOA-Security Guide**: In collaboration with the SOA Working Group, developing a best practice guide to explain what additional security considerations SOA environments demand.
- **Secure Mobile Architectures (SMA) Standard:** Specifying the common technologies for a standards-based SMA solution.Other industry groups involved include the PCI Forum, ARC, SANS Institute, ISA, and TCG-TNC. Application areas include large manufacturing flow lines and safety-critical SCADA environments.
- **Trust Management/Classification Model Guide**: A practical approach describing the essential common levels of sensitivity and classification for the value of data, and effective protection mechanisms to assure secure operation.

SMT

Cloud Security



- Define the appropriate building blocks, roles and use cases that address the appropriate confidentially, integrity and availability requirements of cloud computing

- Develop a Cloud security reference architecture

Cybersecurity – Trustworthy Technology Supplier Framework

What makes a "Good Commercial Product" – Helpful information that builds understanding of the product

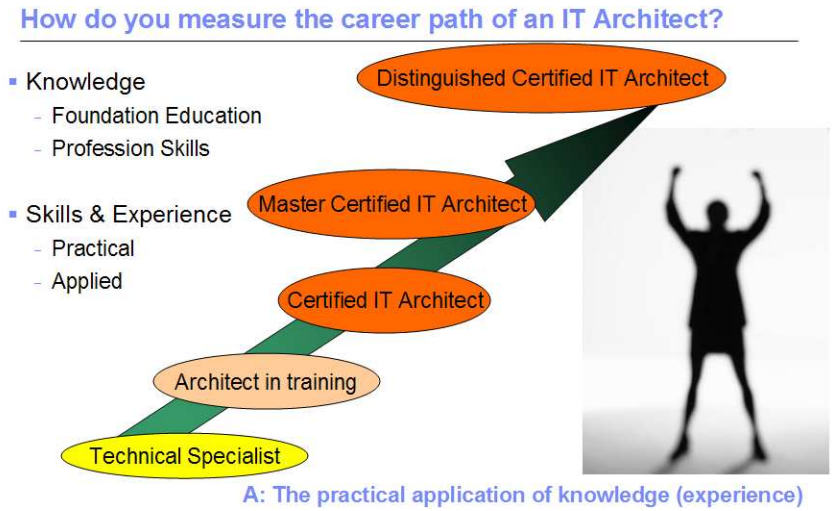
- What's in it (source code and origin/pedigree)
- Who built it (development and manufacturing)
- How will it be sustained from an OEM perspective
- What were the management, process and qu
- What are the meaningful supply chain consic
- What variability, and volatility of sub-process expected (opportunistic component sourcing a
- What other "measures of goodness" can be u
- Not a substitute for ISO, NIST, or ITU; Intero level compliance or certification

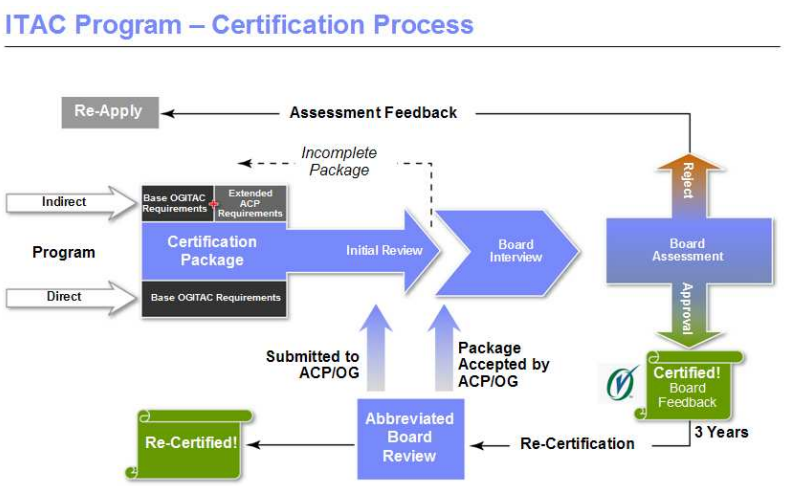
Best Practice Categories	Definition
Product Engineering Method	Trusted Technology Suppliers use a well defined product development or engineering method and/or process. The effectiveness of the method/process is managed through metrics and management oversight.
Secure Engineering / Development Method	Trusted Technology Suppliers employ a secure engineering method in conjunction in support of their product development methods.
Supply Chain Management Method	Trusted Technology Suppliers manage their supply chains through the application of a secure supply chain method / process.

- **Effort to identify industry best practices for**
  - Building trustworthy products
  - Managing trustworthy suppliers

SMT

IT Profession Certification





- Premier IT Architect & IT Specialist Profession Certification
- Accredited companies: EDS, HP, CapGemini, IBM, Rayteon, more…
- More than 2.5K certified architects
- IT Specialist Stream includes Security Architect
- http://www.opengroup.org/itac/ http://www.opengroup.org/itsc

SMT

Software Assurance (SwA) Ecosystem – Standard-based Solution

- OMG focused on core technology standards
- Tooling interoperability standards
- Goal: Standard-based integrated tooling environment that dramatically reduces the cost of multi-disciplinary software assurance activities
- Based on integrated ISO/OMG Open Standards
  - Semantics of Business Vocabulary and Rules (SBVR)
    - For formally capturing knowledge about vulnerabilities
  - Knowledge Discovery Metamodel (KDM)
    - Achieving system transparency in unified way
  - Software Assurance Metamodel: Argumentation Metamodel (ARM) and Software Assurance Evidence Metamodel (SAEM)
    - Intended for presenting Assurance Case and providing end-to-end traceability: requirement-to-artifact
  - Software Metrics Metamodel
    - Representing libraries of system and assurance metrics

SwA Ecosystem is expending: OMG SysA TF developing and integrating standards in area of Threat Risk Assessments and defining Security Vocabulary.

SMT

Harmonizing Gov & Industry Standards Activities – What needs to happen?

- Community-to-Industry Outreach
  - Standardization principles
    - Why do we standardize as an industry
    - Where do we standardize – not all standards bodies are equal
    - Reduce the me-too standards efforts
  - Establish an industry outreach system like
    - FedBizOps
    - Announce interest in industry participation in work groups
- How to Contribute
  - Contribute to the right open standards body
    - Find the authoritative source
    - Example – DMTS for systems management
  - Contribute directly to industry
- Standards Continuity & Integrity
  - Technology Standards should be apolitical (should not be sited in legislature)

SMT